EPMACINST 5520.1C
Code 40D
18 Dec 2001

EPMAC INSTRUCTION 5520.1C

Subj: PERSONNEL SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.30A

1. Purpose. To provide instructions for the administration of Enlisted Placement Management Center's Personnel Security Program.

2. Cancellation. EPMACINST 5520.1B.

3. Background. Reference (a) establishes the basic policy of the Department of the Navy (DON). No person shall be appointed or retained as a civilian employee in the DON; accepted or retained in the Navy; granted a personnel security clearance; assigned to sensitive duties or granted access to classified information; unless appointment, acceptance, retention, clearance, or assignment is clearly consistent with the interests of national security.

4. Policy

a. A determination to grant a security clearance, allow access to classified information or assign an individual to sensitive duties will be based, as a minimum, on a personnel security investigation under the requirements specified in reference (a) for the various levels or kinds of access, position, or duty.

b. Personnel security clearances will be granted on a need to know basis per reference (a) and documented on OPNAV Form 5520/20. For ease of accountability, the Administrative Services Department will publish a security access list containing names of military and civilian personnel holding a clearance. This list will be retained by all departments to ensure only authorized personnel have access to classified information. It should be noted that all Command Duty Officer watchstanders require a secret clearance; therefore, copies of the access list will also be forwarded to the Senior Watch Officer, the Command Duty Notebooks, and Naval Computer and Telecommunications Station, New Orleans.

5. Continuous Evaluation of Eligibility

a. Information reflecting on an individual's reliability and trustworthiness from a security perspective will be reported to the Command Security Manager. All command elements, particularly human resource, security, legal, medical, and supervisory personnel must understand that information which could place an individual's loyalty, reliability, and trustworthiness in question has to be evaluated from a security perspective. Personnel must be alert to behavior indicating unexplained affluence, financial instability, alcohol and drug abuse, mental or emotional instability, or criminal conduct that is potentially significant to an individual's security status. Supervisors should act to identify problem areas at an early stage and direct personnel to programs designed to counsel and assist them when they are experiencing financial, medical, or emotional difficulties.

b. Co-workers have an equal obligation to advise their supervisor or appropriate security officials when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

c. When derogatory or questionable information is acquired about an individual who holds a security clearance or assignment to sensitive duties, the appropriate determination authority must reevaluate the individual's eligibility for access or assignment. The Command Security Manager will make a recommendation to the Commanding Officer (CO), via the Executive Officer, upon initial receipt of credible derogatory information whether to suspend access to classified information and/or continue assignment to a sensitive position, pending final decision by the appropriate determination authority. The CO will determine whether, on the basis of all the facts available upon receipt of the initial derogatory information, if it is in the interest of national security to take interim action to suspend or limit an individual's access to classified information or reassign the individual to nonsensitive duties until a final determination is made. The Department of the Navy, Central Adjudication Facility will suspend access for civilian employees, if not already accomplished by the command, when a letter of intent to revoke a security clearance is issued.

d. Supervisors will comment on eligibility of persons for continued access to classified information and discharge of security responsibilities in conjunction with regularly scheduled performance appraisals of military and civilian personnel whose duties entail access to classified information.

e. A security clearance which was administratively withdrawn or lowered may be reinstated to the previous level of eligibility if access requirements for official duties so warrant.

6. Responsibilities

a. Command Security Manager

(1) Is the principal advisor on security in the command and is responsible to the CO for the management of the program.

(2) Ensures written command personnel security procedures are maintained.

(3) Ensures personnel security orientation, debriefing, education, and training are accomplished.

(4) Ensures that individuals are not granted access to classified material until the required documentation, commensurate with the level of access, has been completed.

(5) Performs all other duties as listed in reference (a).

(6) Ensures all reporting and detaching military personnel have documentation in their service record of appropriate level of investigation for assignment. Assists the individual in preparation of necessary documents to request an investigation.

(7) Signs OPNAV Form 5520/20 and OPNAV Form 5510/413, Personnel Security Action Request, and ensures follow-up actions are taken, if needed.

(8) Ensures original OPNAV Form 5520/20 is filed in the individual’s service record. Maintains a pending and completed file of all OPNAV 5520/20 and OPNAV 5510/413 forms.

(9) Ensures that all military and civilian personnel who are to handle classified information or to be assigned to sensitive duties are appropriately cleared and that requests for personnel security investigations are properly prepared, submitted, and maintained. Ensures Department of Defense military and civilian personnel complete and sign an SF 312, before being given initial access to classified material.

(10) Ensures that an individual's personnel security investigation, clearance, and access are recorded.

(11) Publishes a security access list quarterly or more frequently as circumstances dictate.

(12) Ensures Single Scope Background Investigations (SSBI's) are updated as needed or required.

b. Department Heads. Department Heads will review the security access list to determine changes and report the changes to the Command Security Manager.

7. Forms. OPNAV Form 5520/20 (Rev. 10-79) Certificate of Personnel Security Investigation, Clearance and Access; SF 312 (Rev. 1-91), Classified Information Non-disclosure Agreement; and OPNAV Form 5510/413 (Rev. 4-90), Personnel Security Action Request, are stocked in the Administrative Services Department.

G. SHEEHAN

Distribution:
EPMAC Intranet